Abstract:	This document provides information concerning CSRICs actions in response to incident INC000002665039 SEC-14581
AAR Title:	After Action Report: *NCCIC INC10219396 Sensitive But Unclassified Data Exposure on EPA.gov*
AAR Date:	November 9, 2018
Incident Date:	September 26, 2018
AAR Owner:	(b) (6), CSIRC Incident Response Team Lead
AAR Author:	Senior Incident Response Analyst (b) (6)
AAR Approved by:	(b) (6)
Approved date:	September 12, 2019

Document History

Version	Date	Author	Description of Change	Approved by
1.0	10 Jan 2018	(b) (6)	Initial template release.	(b) (6)

Table of Contents

1. Incident ID and Description

Incident Ticket	INC000002665039 - *Sensitive But Unclassified Data Exposure on EPA.gov*
09/26/18 6:00 pm	CSIRC received a notification from (b) (6) (Treasury) that sensitive but unclassified information was publicly available from web search on epa.gov.

2. Actions Taken

Date	Actor	Description
09/26/18 6:30pm	(b) (6)	CSIRC contacted (b) (6) (Middleware) informing her of the report.
09/26/18 6:35pm	(b) (6)	CSIRC contacted console operations. Requested after hours phone for Hosting. CSIRC was given (b) (6) Number as on call 919-599-2592. (b) (6) confirmed Middleware and (b) (6) as the contact for epa.gov site.
09/26/18 6:47pm	(b) (6)	CSIRC notified OEI ISO of the incident.
09/26/18 7:00pm	(b) (6)	Actions Taken by (b) (6): I have spoken to one of the www.epa.gov customers, (b) (6). He asked that we do two things: • Remove the file from the Akamai site cache. In progress • That we remove the file from the origin server as well. In progress
09/26/18 7:14pm	(b) (6)	CSIRC notified Breach Team of the incident.
09/26/18 7:19pm	(b) (6)	CSIRC notified US-CERT of the incident.
09/26/18 7:37pm	(b) (6)	(b) (6) spoke with (b) (6) regarding the other questionable file that was accessible. She requested that file be removed as well. Spoke with (b) (6) by phone and confirmed both files had been removed.
09/27/18 10:47am	(b) (6)	CSIRC's sent an update email to (b) (6).

3. Resulting Condition

Condition	Description
Sensitive but Unclassified Data Exposure on EPA.gov	One main issue discovered: 1) A basic Google search for "Fiscal Service Security Plan" on epa.gov would return an ISA with EPA/TWAI proprietary information. During the investigation a second file was found to be sensitive in nature. The files in question were confirmed to have been removed on 09/26/18 at approximately 7:30pm

4. Lessons Learned

Control	Lesson	Description
Secure Configurations for Hardware and Software. **CM**	Sensitive data present on public site	The lack of a system or process to check external public facing Web sites was the cause of this incident.
Recommendations		
The implementation of a Data Loss Prevention (DLP) system to perform scans of all external (public facing) Web servers to check for Controlled Unclassified Information (CUI) and Personal Identifying Information (PII).		
The Agency should review and assess current change control process and policy, to ensure both process and policy meet Agency's security standards.		

Control	Lesson	Description
Inventory of Authorized and Unauthorized Device. **CM**	Missing list of system owners/POC's	The delay in remediation was primarily because there is not a source of well-defined system owners.
Recommendations		
The Agency should compile, maintain, and make available to CSIRC, the Agency's complete asset inventory list. Along with asset value, associated applications and software, POC's, and Region/Program Office affiliation.		